PALADION
HIGH SPEED CYBER DEFENSE

MAZE RANSOMWARE ADVISORY

How to protect your business from the Maze Ransomware, and everything we know about this Malware

While Maze is not a new ransomware, it is an extremely deadly one. It was among the first ransomware to use "double extortion" tactics to extort victim organizations. Traditional ransomware attackers never hosted their websites or openly engaged in Twitter. They have firmly established a reputation of first stealing data before locking their target systems. By fully understanding their victim's reputational risks, their now infamous system of 'steal, lock and extort" has become commonplace in the cyberspace.

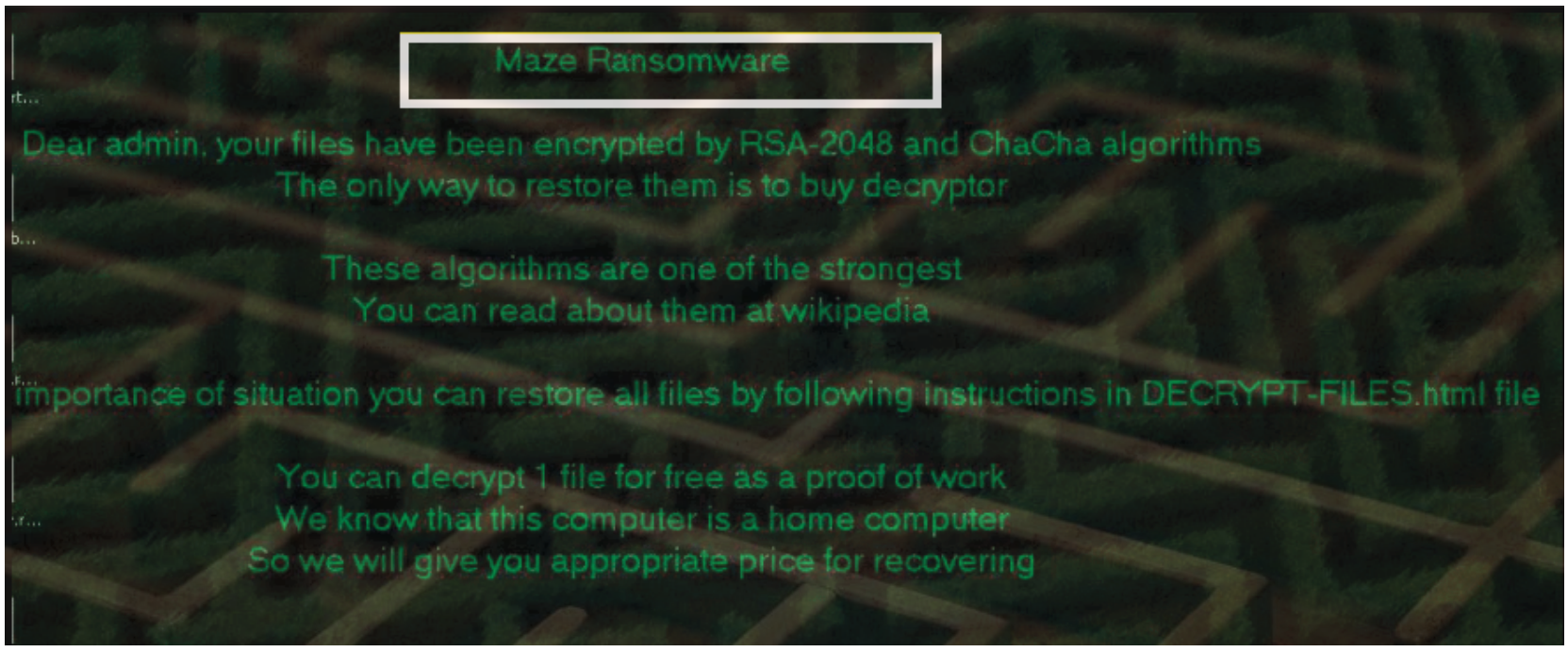
Attacks such as this, have increased exponentially in the current COVID-19 landscape. With higher vulnerabilities caused by a decentralized workforce and the resultant scramble to adapt to keep operations running, businesses are at higher risk than ever before. Careful yet swift measures must be taken to protect against the Maze ransomware, and a plethora of others to avoid massive financial and reputational damage.

What is its Impact? Why you need to worry

- Even if you have a backup, you are not entirely safe from Maze. While the primary goal of the ransomware is to encrypt all files in an infected system and then demand a ransom to recover the files, the most worrying impact of Maze is the threat of data being released on the internet if the victims don't pay up.
- It disrupts the services of targeted organizations and possibly puts their customers in danger as well.
- In most cases, the costs of self-recovery exceed ransom demands. As an example, an organization refused to pay $80,000 in ransom and, as a result, suffered damages of $18,000,000 in remediation, new hardware, and loss of revenue. This has led to some insurance companies recommending that the victims just pay the ransom.
- Other damages to organizations include downtime, share price depreciation, the technical cost of system and data recovery, ransom payment, and more. Most of the time, targeted victims do not publicize the attack due to the resulting dent in brand reputation.
- Data breaches occurring from these ransomware attacks, expose their victims to loss of proprietary information, and also hinders their ability to protect clients' and employees' personal information. Stolen data can be used for future attacks on those whose details were included in the breach. Regulatory laws like the European Union GDPR, mandate that victims of such attacks must disclose the details of the attack both to specific authorities and corporations and individuals to whom the information belongs. This includes the list of potential damage and additional costs needed for the protection of employees and customers from fraud and identity theft, as well as exposure to potential lawsuits.
- Maze attackers can use the exfiltrated data to launch subsequent targeted attacks like phishing (even if you pay and get the unlock key for them not to make that data public).

How to protect yourself?

- Backup files: Continuously back up files in different formats to multiple locations. This measure will help you recover data in case of a ransomware attack. Design a procedure document for backups or review existing documentation.
- Develop Playbooks to tackle ransomware: This will help you with step by step details of activities to be performed to mitigate such attacks. This needs to be developed with the consideration of both technical and governance aspects.
- Vulnerability Patching: Regularly patch up vulnerabilities on applications and systems, that are specific to maze ransomware exploit kits. One of the exploit kits Maze uses is called Fallout, which utilizes various exploits found on GitHub. One of these vulnerabilities is a Flash Player exploit, CVE-2018-15982. Fallout is a relatively new exploit kit that uses PowerShell instead of the web browser to run its payload. Maze has also been observed using Spelevo, another exploit kit.
- Security awareness: Perform a people risk assessment to understand the level of security know-how of end-users and how they would react if they received phishing emails with embedded Malware in standard attachments. Develop and distribute awareness content to end-users, especially on socially engineered emails.
- Continuous Compromise assessments: Perform regular assessments on endpoints and servers to check if the organization is vulnerable or could be susceptible to similar ransomware. This will also enable organizations to hunt for hidden Malware, trojans, or backdoors, which evade detection by traditional technologies.
- Reach out to your SOC vendor, who can provide IOCs that can help detect traces of Maze ransomware within your environment.
- Anti-Phishing Services: Subscribe to Anti Phishing services, which also provides Dark web monitoring. This will alert you within the case that your data is already floating on the Dark web. It will also help you with data loss recovery.
- Use machine learning techniques to identify data exfiltration attempts. As Maze exfiltrates data before encrypting files, this can be an early indicator to stop the attack.



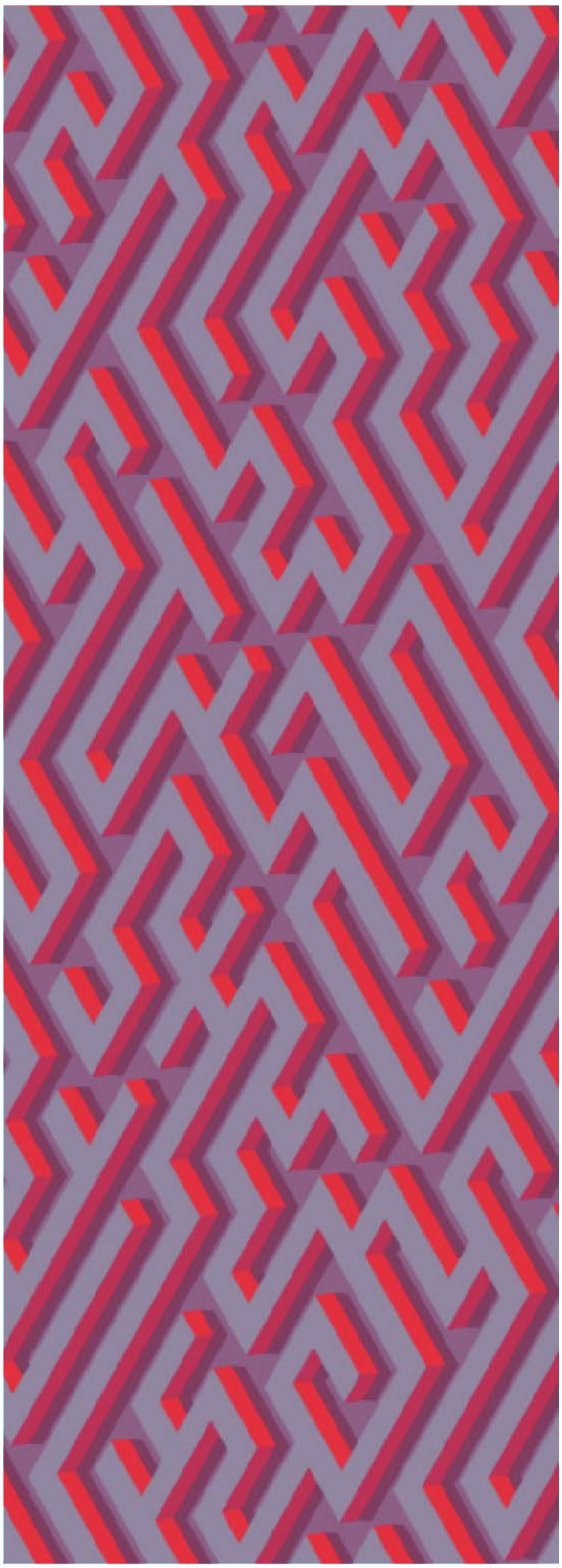
Additional Details about Maze Ransomware

What is Maze Ransomware?

Earlier known as ChaCha ransomware, Maze was discovered in May 2019 by Jerome Segura, a malware intelligence analyst. "Maze is a ransomware created by skilled developers," McAfee noted in its examination of the code that: "It uses a lot of tricks to make analysis very complex by disabling disassemblers and using pseudocode plugins."

Differentiating itself from other Malware, Maze began publicly listing its campaign victims by posting the names of the companies that have not complied with their ransom demands. Attack campaigns employing Maze typically pose as legitimate government agencies and security vendors to steal and encrypt data to then attempt to extort the data owner.

Interpol has also alerted health organizations across the world to prepare themselves for possible attacks involving dangerous ransomware. Even though the Maze ransomware group has reportedly been on record that they will not be targeting healthcare and medical facilities for the time being. Breaking this 'assurance,' they struck drug testing firm "Hammersmith Medicines Research LTD [HMR]," a London-based company that carries out clinical trials for new medicines and that is on standby to perform live trials of Coronavirus vaccines. The attack took place on the 14th of March 2020, when the "Maze" ransomware operators exfiltrated data from the HMR's network and then encrypted their systems.



How does it function?

Attackers use Maze as part of a Multi-layer cyberattack. Of late, Maze is being observed appearing in the second or third step of these campaigns and is less likely to be used as an initial access technique. Maze ransomware generally uses 2048 bit "Rivest-Shamir-Adleman" (RSA) and the "ChaCha20" stream cipher to encrypt individual files.

Below are some details about how it functions:

1. The Malware has previously used different techniques to gain entry onto a victim machine, mainly using exploit kits, remote desktop connections with weak passwords, or via email impersonation.

2. The malicious emails generally come with a Word attachment that uses macros to run the Malware in the system.

3. Exploit kits used by Maze include "Fallout" and "Spelevo" and are also known to exploit the vulnerability (CVE-2018-15982) in the Flash Player.

4. The Malware is hard programmed by the authors with some tricks to prevent its reverse. This makes static analysis by researchers more challenging.

PALADION

HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a next-generation cybersecurity provider to technology, manufacturing, and cloud-first companies across the United States. They are consistently recognized and rated by independent technology advisory firms for their Managed Detection and Response Services, Cloud security, and Vulnerability Management & Response services, which is anchored by their patented Artificial Intelligence platform – AIsaac.

For more information, please visit http://www.paladion.net.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-703-956-9468
India: +91-80-42543444, UAE: +971-4-2595526
Sales@paladion.net